UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/596,652	06/19/2000	THOMAS A BERSON	XER1P002	4307

7590 05/03/2004

Patent Documentation Center
Xerox Corporation
100 Clinton Avenues., Xerox Sq. 20th floor
Rochester, NY 14644

EXAMINER
GURSHMAN, GRIGORY

ART UNIT	PAPER NUMBER
2132	8

DATE MAILED: 05/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/596,652	**Applicant(s)** BERSON ET AL.
	Examiner Grigory Gurshman	**Art Unit** 2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on *08 April 2004*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-15 and 17-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3, 5-15 and 17-22* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 November 2003* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *6, mailed 1/20/04*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Drawings

1. Additional drawings Figures 1A, 1B and 1C are accepted by examiner.

Response to Arguments

2. Applicant's amendment of claims 1, 3, 5-9, 13, 15,17-21 reflects replacing the term "work" with that of "cryptographic service". This limitation is addressed in the claim rejections herein.

3. Regarding the remaining claims 1-3, 5-15 and 17-22, Applicant argues that McGravey does not teach off-loading of a cryptographic service from a client to a server. Examiner points out that while McGravey does not explicitly teach "off-loading of a cryptographic service", it is not recited in Applicant's claims.

4. Applicant further argues that nothing in McGravey teaches a suggestion to modify McGravey to include a network server that provides cryptographic services.

Examiner respectfully disagrees and points out that McGravey himself teaches providing cryptographic services at the server (see Fig.6). McGravey teaches that the session key(s) are sent 607 (in Fig. 6) from the private key system to the server to enable the server to decrypt data requests coming in from the client and to encrypt the resulting messages to the client (see column 10, lines 33-36), which meets the limitation "cryptographic services".

Examiner also points out that while McGravey states that the server tunnels all the client information on to the private key system as shown at 602, McGarvey does not explicitly teach generating a tunnel on the network and utilizing the tunnel for sending information form the client to the server. Kirby discloses transferring encrypted packets over a public network (see abstract). Kirby teaches that the policy id field is used to create tunnels 140, 142 between firewall computers 146, 148 on internet 152 (see Fig.8). When computer 146 receives a network packet, it checks the policy id to determine which "tunnel" the packet came through. The tunnel indicates the type of encryption algorithm used to encrypt the packet (see column 5, lines 36-42).

Examiner maintains that one of ordinary skill in the art would have been motivated to receive information at the server from the client utilizing the tunnel as taught in Kirby for determining the type of encryption algorithm used to encrypt the packet (see Kirby column 5, lines 36-42). Therefore the combination of teachings of McGravey and Kirby renders the instant claims obvious.

5. The rejections of remaining claims are maintained .

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 5-15 and 17-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over McGravey (U.S. Patent No. 6.643.774 B1) in view of Kirby (U.S. Patent No. 5.898.784).

7. Referring to the instant claims, McGravey discloses a method for delegating authority in a public key authentication environment from a client to a server machine or process, in order that the server machine or process can then securely access resources and securely perform tasks on behalf of the client (see abstract). McGravey shows in Fig. 6 that the client sends an initial request at 601, comprising a nonce (nonce1) and a request for the server's certificate. The server forwards or tunnels all the client information received from the client during the handshaking process on to the private key system as shown at 602. The private key system now has the nonce1 (from the client), and the original request from the client. The private key system responds 603 by sending a signed nonce1, a nonce2, and the private key system's certificate (identified in FIG. 6 as the security certificate) to the server. The server then forwards 604 this information to the client. The client then responds 605 by sending a signed nonce2 and the client certificate to the server. The server forwards 606 or tunnels this information to the private key system.

8. Referring to the independent claims 1, 13 and 20, the limitation "identifying a client utilizing the network" is met by the client, which sends an initial request at 601, comprising a nonce (nonce1) and a request for the server's certificate (see Fig.6). The limitation "receiving information at the server from the client ... wherein the information is encrypted by the client using the first key and performing cryptographic service at the server" is met by the private key system (i.e. client connected to the server) sending a signed nonce1, a nonce2, and the private key system's certificate (identified in FIG. 6 as the security certificate) to the server. While McGravey states that

the server tunnels all the client information on to the private key system as shown at 602, McGarvey does not explicitly teach generating a tunnel on the network and utilizing the tunnel for sending information form the client to the server.

Referring to the instant claims, Kirby discloses transferring encrypted packets over a public network (see abstract). Kirby teaches that the policy id field is used to create tunnels 140, 142 between firewall computers 146, 148 on internet 152 (see Fig.8). When computer 146 receives a network packet, it checks the policy id to determine which "tunnel" the packet came through. The tunnel indicates the type of encryption algorithm used to encrypt the packet (see column 5, lines 36-42). Therefore, at the time the invention was made, it would have been obvious to one of ordinary skill in the art to receive information at the server from the client of McGravey utilizing the tunnel as taught in Kirby. One of ordinary skill in the art would have been motivated to receive information at the server from the client utilizing the tunnel as taught in Kirby for determining the type of encryption algorithm used to encrypt the packet (see column 5, lines 36-42).

9. Referring to claims 3, 15 and 21, McGravey teaches sending a signed nonce1, a nonce2 (see Fig.6), which meets the limitation "key comprises at least one parameter for the cryptographic service performed by the server".

10. Referring to claims 5, it is well known in the art to perform modular exponentiation at the server. One of ordinary skill in the art would have been motivated to perform modular exponentiation at the server in order not to reveal the client secret to the server.

11. Referring to claims 6 and 18, "transmitting the cryptographic service result to the client" is met by the server, which sends 610 the session credential and a request for the ticket(s) to the private key system (see Fig.6).

12. Referring to claim 22, it is well know in the art to have the message blinded by the user before transmittal to the server. One of ordinary skill in the art would have been motivated to have the message blinded prior to transmission for security in case of interception.

Conclusion

13. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Grigory Gurshman whose telephone number is (703) 306-2900. The examiner can normally be reached on 9 AM-5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the TC 2100 receptionist whose telephone number is (703) 305-3900.

Grigory Gurshman
Examiner
Art Unit 2132

G.G.

GG
April 27, 2004

Gilberto B

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100